**IT Applications Unit 3, AOS 1, Online Communities**

1. Complete the following, from pgs, 32: **Network security**

**Networks are classified according to below and we will study the following:**

1. Network Categories: LAN, WAN
2. Network Architecture, client-server; peer-to-peer; internet peer-to-peer; intranet
3. Network communication standards
4. Network hardware and software
5. Transmission media
6. **Network security**
7. What types of physical security measures can be put in place?

Physical security measures, such as locks and alarms to warn of intruders, can protect a cabled network to a degree, but it cannot protect it from attack over the internet. a wireless network must employ additional security, since the nature of radio wave transmission is that its range is often beyond the boundaries of an organisation’s property.

**Usernames and passwords**

1. Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.

Be at least 8 digits, include non-alphabetical characters, not be easily guessed, be changed every month.

**Firewall**

1. Describe the nature of a firewall.

A firewall is a server and software combination that filters the information coming through an internet connection into an organisation’s internal network. Any packet of data that is flagged by the filters as unwanted is not allowed through.

1. What are the main purposes of firewalls and how are these purposes achieved?

The filters used by a firewall include examining the IP address of computers that request information from an internal server, blocking all access to certain domain names, banning certain protocols (e.g. file transfer protocol, mail protocol or telnet protocol) from accessing particular servers, and certain words and phrases included in packets of information. A firewall can also be used to restrict employees’ access to sensitive information. For example, a firewall can be used to stop some personnel from accessing the payroll database.

1. Why do firewalls use 2 separate NICs?

Most firewalls use two separate NICs; one is connected to the internal network and the other to the outside world. Material can only move from one card to the other through the CPU of the server computer that is acting as the firewall.

**Malware protection**

1. What is malware and what strategies are used to protect against this type of software?

Malware refers to malicious software and includes spyware, adware, Trojan horses, worms and viruses. Network administrators usually require workstations to run virus protection software. The antivirus software is often updated automatically via the network. A firewall is also useful to block malware from sending personal information over the internet. Anti-adware programs should also be run on workstations.

**Encryption**

1. What is encryption?

Encryption is the process of translating data into a secret code that can only be read by authorised users. To read an encrypted file, you must have access to a secret key that you can use to decrypt the data.

1. Describe the nature of WPA or WPA2.

Wi-Fi protected access (WPA or WPA2) is a security protocol for use by wireless LANs. It provides security by encrypting data sent over radio waves so that is it protected during transmission from the sending device to the receiving device. WPA is designed to provide the same level of security to wireless environments as that of a wired network.

1. What is encrypted data known as?

Encrypted data is referred to as cipher text.

**Secure Websites**

1. Describe the secure protocol to allow secure financial transactions across the internet.

Websites that allow financial transactions use the industry standard hypertext transfer protocol security (https) as the secure protocol between a client’s web browser and the web server, to ensure that a secure connection is established and maintained.

1. What is digital identification certificate technology based on?

Digital identification certificate technology is based on a trusted certificate authority such as VeriSign Incorporated.

1. Describe the nature of Secure sockets layer (SSL) protocol.

Secure sockets layer (SSL) is a cryptographic protocol that provides secure connection on the internet. When a web browser points to a secured domain, a SSL ‘handshake’ authenticates the server (website) and the clients (web browser).

**Physical design of networks**

1. What is the role of a network diagram?

Networks in medium to large organisations can become very complex, with servers, workstations, printers and cables spread widely throughout the premises. Technical support people need a method of representing the network and all of its different pathways that provides an overview of the connections and allows them to identify and locate equipment.